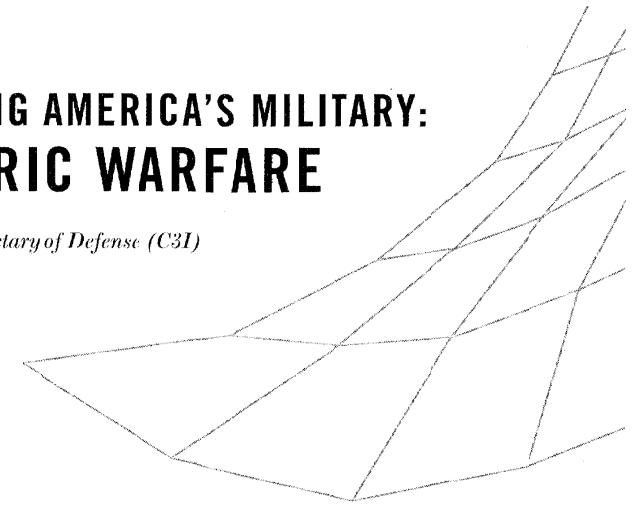


THE GOAL

“Net-centric warfare” comes down to this: harnessing the collaborative behavior that results from ever-faster access to information. In military terms, this means the creation of a Global Information Grid that uses technology to get more and better information to people in the field so they can collectively act on it to accomplish their assigned missions in ways heretofore impossible. It means robust, reliable command and control. It means pushing more power to the edges of our armed forces by providing ready access to information, rather than filtering it through stove-piped channels. Finally, it means building an organization agile enough to effectively accommodate the unknown. There’s less time than ever to mass heavy forces. There are fewer ways to build a supply chain. Foes are indifferent to normal rules of engagement. In these circumstances, information technology – and related collaboration – can help guarantee our continued military superiority. Net-centric warfare is America’s competitive advantage of the future.

TRANSFORMING AMERICA’S MILITARY: NET-CENTRIC WARFARE

Office of the Assistant Secretary of Defense (C3I)



What NCW *Doesn't* Mean

What NCW Means

Sources of information decide what users need
Users of information access what they need

Centralized chain that can be cut or broken
Robust networks without a central weakness

Multiple “stovepipe” comms. infrastructures
Interoperable communications infrastructure

Totally unrestricted information
More information, gathered in smarter ways

Trying to contain information that exists
Doing more with information that exists

Task, Process, Exploit, Disseminate (TP&ED)
Task, Post, Process, Use (TPPU)

Fixed – domain specific – security
Dynamic – or situational – security

Totally autonomous operations
Self-synchronizing operations

Best-time-possible hierarchical comma
Real-time collaboration

Push (broadcast) information out
Pull information down

Bandwidth constrained
Bandwidth as needed

Cycle-time in hours
Cycle-time in seconds

Risk avoidance
Risk management

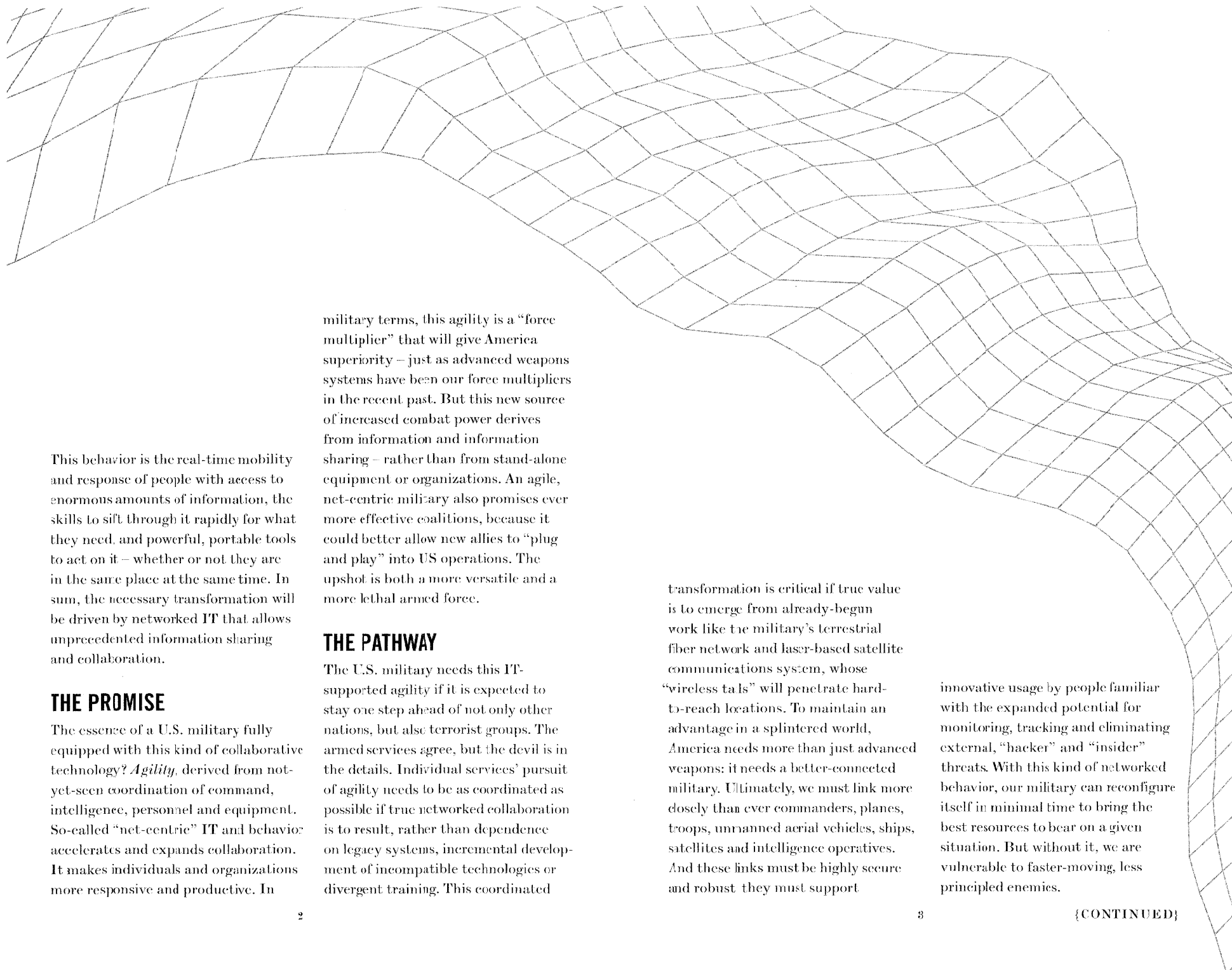
Circuits
Packets

THE THREAT

All Americans are now awake to an unpleasant new reality. We saw hints of it for a decade: conflicts in Bosnia and Kosovo; the 1993 World Trade Center bombing; and the 2000 assault on the USS Cole. The terrorist attacks on 9/11 and operations in Afghanistan brought this reality into sharp focus. The Cold War world with a monolithic enemy is gone, along with its shared, if opposed, concepts of conflict. In its place is the simmering, unpredictable threat of religious and ethnic warfare, terrorism, and potential aggression by states like Iraq and North Korea – all with a proven or potential willingness to use unconventional methods to harm the U.S. America is correctly adjusting its foreign policy and homeland security apparatus in response. But it also needs to transform its military.

THE MEANS

The key to this transformation: information technology (IT). Since the Gulf War, military technology has focused largely on “smarter” bombs and more advanced weapons systems. But the splintered reality of today’s conflicts calls for farther-reaching improvements. It requires an overall transformation, where technology drives greater real-time mobility and response throughout all our armed forces. This “Information Age” change must reflect the productive, networked interaction that millions of Americans already demonstrate through mobile use of email, peer-to-peer file sharing, cell phones, web-conferencing, chat boards and search engines – behavior that, e.g., lets businesses turn on a dime to seize market opportunities as they develop, not after they come to fruition.



This behavior is the real-time mobility and response of people with access to enormous amounts of information, the skills to sift through it rapidly for what they need, and powerful, portable tools to act on it – whether or not they are in the same place at the same time. In sum, the necessary transformation will be driven by networked IT that allows unprecedented information sharing and collaboration.

THE PROMISE

The essence of a U.S. military fully equipped with this kind of collaborative technology? *Agility*, derived from not-yet-seen coordination of command, intelligence, personnel and equipment. So-called “net-centric” IT and behavior accelerates and expands collaboration. It makes individuals and organizations more responsive and productive. In

military terms, this agility is a “force multiplier” that will give America superiority – just as advanced weapons systems have been our force multipliers in the recent past. But this new source of increased combat power derives from information and information sharing – rather than from stand-alone equipment or organizations. An agile, net-centric military also promises ever more effective coalitions, because it could better allow new allies to “plug and play” into US operations. The upshot is both a more versatile and a more lethal armed force.

THE PATHWAY

The U.S. military needs this IT-supported agility if it is expected to stay one step ahead of not only other nations, but also terrorist groups. The armed services agree, but the devil is in the details. Individual services’ pursuit of agility needs to be as coordinated as possible if true networked collaboration is to result, rather than dependence on legacy systems, incremental development of incompatible technologies or divergent training. This coordinated

transformation is critical if true value is to emerge from already-begun work like the military’s terrestrial fiber network and laser-based satellite communications system, whose “wireless tails” will penetrate hard-to-reach locations. To maintain an advantage in a splintered world, America needs more than just advanced weapons; it needs a better-connected military. Ultimately, we must link more closely than ever commanders, planes, troops, unmanned aerial vehicles, ships, satellites and intelligence operatives. And these links must be highly secure and robust: they must support

innovative usage by people familiar with the expanded potential for monitoring, tracking and eliminating external, “hacker” and “insider” threats. With this kind of networked behavior, our military can reconfigure itself in minimal time to bring the best resources to bear on a given situation. But without it, we are vulnerable to faster-moving, less principled enemies.